Recommendation-based Trust Model for Vehicle-to-Everything (V2X)

Aljawharah Alnasser, Hongjian Sun, *Senior Member*, *IEEE* and Jing Jiang, *Member*, *IEEE*

***Abstract*—Intelligent Transportation System (ITS) is one of the main systems which have been developed to achieve safe traffic and efficient transportation. It enables the vehicles to establish connections with other road entities and infrastructure units using Vehicle-to-Everything (V2X) communications. As a consequence, all road entities become exposed to either internal or external attacks. Internal attacks cannot be detected by traditional security schemes. In this paper, a recommendation-based trust model for V2X communications is proposed to defend against internal attacks. Four types of malicious attacks are analysed. In addition, we conduct various experiments with different percentage of malicious nodes to measure the performance of the proposed model. In comparison with the existing model, the proposed model shows an improvement in the network throughput and the detection rate for all types of considered malicious behaviors. Our model improves the Packet Dropping Rate (PDR) with 36% when the percentage of malicious nodes is around 87.5%.**

***Index Terms*—Trust, V2X, Recommendation, Attack.**

I. Introduction

THE transportation industry has received a massive evolution during the last few years. The automotive companies have worked on combining hardware and software into their vehicles to make them smarter. Thus, the vehicles become able to communicate and interact with the surrounding environment. Intelligent Transportation System (ITS) is the key enabler of smart cities where the communication is supported between road entities such as buses, pedestrians, motorcycles and cycles, which is called Vehicle-to-Everything (V2X) communication.

V2X supports a unified connectivity platform for the road entities. Each road entity is able to share information such as speed, direction, and location with the surrounding entities. In case of sudden events such as accidents or congestion, an alarm message is sent to warn the neighboring entities. The communication type depends on the entities that establish the link. V2X supports five types of communications which are Vehicle-to-Sensors, Vehicle-to-Vehicle, Vehicle-to-Pedestrian, Vehicle-to-Grid and Vehicle-to-Infrastructure [1]. The interoperability among heterogeneous devices is one of the main challenges in V2X communication. As a consequence, 3GPP group released LTE protocol (Release 14) to support V2X services.

Indeed, static users have more stable connection and static network topology. On the other hand, mobile nodes have challenge in choosing next hop where the network topology is frequently changed. Also, the communication time between road entities is limited. The ad-hoc link between road entities is more exposed to external or internal attacks than the cellular connection because it is not managed by the Core Network (CN) [2]. *External attacks* are initiated by unauthorized nodes in the network. It could happen when two entities are located out of the network coverage; then, there is a possibility of communicating with a revoked entity. *Internal attacks* are launched by authorized nodes which have valid credentials. Indeed, internal attackers break through some traditional security measures such as cryptography and authentication [3][4] because the road entity is usually authenticated but users can tamper with the nodes for malicious activities [5]. In addition, transaction messages must be protected and forwarded directly to the CN because they have personal and confidential data [6]. Also, they could be sent through a multihop route to the CN. However, the relaying node could be an internal attacker that stops the packets forwarding process. Therefore, it affects the network performance adversely.

As a consequence, a trust-based model was suggested to detect internal attackers by monitoring the neighbors' behavior and collecting information about them [3]. Then, this information could be sent to other neighbors as a recommendation or to central units as an alarm. Recently, some researchers designed trust models for vehicular networks to build up trust relationships among nodes. For instance, Chuang and Lee [7] applied trust model as an authentication scheme where the vehicle is considered trusted when it is successfully authenticated. However, the model is able to detect external attackers only. In addition, Shen *et al.* [8] implemented a message authentication scheme where some vehicles are known as verifiers. The verifier vehicles check the validity of the received messages and send their decisions to non-verifier vehicles to guide them for accepting or rejecting the message. In addition, the proposed framework in [9] provided three security measures to ensure the message's trustworthiness. It checks that the message was generated from a trusted location and followed a trusted path. Also, it checks the validity of the message's content. Mrmola and

A. Alnasser is with the Department of Information Technology, King Saud University, Riyadh, KSU, 11543, e-mail: alalnasser@ksu.edu.sa, and also with School of Engineering and Computing Sciences, Durham University, Durham.

H. Sun is with the Department of Engineering, Durham University, Durham, UK, DH1 3LE, e-mail: hongjian.sun@durham.ac.uk.

J. Jiang is with the Department of Mathematics, Physics and Electrical Engineering, Northumbria University, Newcastle upon Tyne, UK, NE1 8ST, e-mail: jing.jiang@northumbria.ac.uk

This work was supported by the UK EPSRC under Grant EP/ P005950/1, and in part by the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 734325 TESTBED project.

Manuscript accepted on 24th October, 2019.

Prezb [10] designed a security model that works on detecting selfish nodes that transmit false or bogus messages. The model defined a fuzzy set to classify each node with three different trust levels. Based on the source node trustworthiness level, the receiver can decide whether it has to receive, forward or drop it. In these solutions, the node can only make a decision when there is a previous communication with the considered node. However, this is not the case in vehicular network where there is always high chance for meeting new nodes.

To address new nodes problem, recommendation-based trust model was suggested where the decision is based on direct interactions and the received recommendations. However, in some cases, the compromised node sends a fake recommendation regarding a normal node or other malicious node. As a result, adding recommendation filtering phase to the trust model was developed to ignore dishonest recommendations. For instance, Hu *et al.* [11] suggested a recommendation-based trust model for choosing a trusted node as a platoon head. They took various trust attacks into consideration such as bad-mouthing, newcomers, and on-off attacks. It is a centralized model where all trust values and feedback regarding their trips are sent to Road Side Units (RSUs). However, the accuracy decreases in the areas where there is no RSUs. Furthermore, Zhou *et al.* [12] applied trust model as a security authentication method. Based on the computed trust value, the node is granted the access to the network. The model is composed of two trust components: direct trust and indirect trust. However, the node only ignores the fake recommendations that are sent by nodes with low trust values. Also, Ahmed and Tepe [13] implemented a trust model to identify and ignore malicious recommendations. The model included a similarity model to determine whether the recommendation is true or not. The evaluating node computes the similarity between its opinion and the received recommendations. The main drawback of this model is that the node cannot measure the similarity when it does not have an opinion regarding that node. Thus, it should have direct interaction with that node to be able to provide its opinion.

To overcome some of these limitations, this paper proposes a distributed recommendation-based trust model for protecting direct links in the V2X network. The node can make a decision independently and detect malicious nodes prior to interactions. In addition, the proposed model is able to ignore the dishonest recommendations that are generated by highly trusted nodes. Furthermore, we study the impact of non-stable malicious behavior on the proposed model. Also, we analyse the performance of the proposed model in comparison with the existing model in [14]. In brief, the main contributions of this paper are:

1) This paper proposes a recommendation-based trust model for V2X communication. Different from existing research, it is a distributed model that targeting at non-stable malicious behavior.
2) Adaptive weights are applied in the recommendation filtering process. The weights are changed based on the number of positive and negative recommendations. Thus, the effect of the recommendation attacks is reduced.
3) This paper compares the performance of the proposed model with the existing model in [14]; our model improves the Packet Dropping Rate (PDR) with 36% when the percentage of malicious nodes is around 87.5%.

The paper is organised as follow. Section II proposes the system model for the V2X network. Section III illustrates the proposed trust model. Section IV shows the simulation analysis for the proposed model. Section V provides theoretical analysis for the proposed model. Section VI presents the comparison results with the existing model. Finally, Section VII summarises the overall work performed.

II. Proposed System Model

A. The considered network

The considered network is a vehicular network which consists of N road entities. The road entities move at random speeds through a dedicated route. Here, we use "node" and "road entity" interchangeably for the same meaning. The transaction message is sent to the CN for further analysis. In the relay coverage scenario, the communication between two road entities is established when one of them is located out of network coverage. The communication forms a multi-hop route to deliver the packets to the CN. We consider two types of nodes as follows:

1) Normal node: It keeps monitoring the surrounding environment and sends its packets to the CN. Also, it relays any received packets to the nearest RSU.

2) Malicious node: In the considered scenario, the relaying nodes could be compromised nodes that launch the following attacks:

- **Routing attacks** which affect the packet routing such as Blackhole attack where the compromised node drops all of the received packets [15]; and Greyhole attack where the compromised node drops some of the received packets [16].
- **Recommendation attacks** where the compromised nodes send fake recommendations to destroy trust decision [17] such as Bad-mouthing attack where the malicious node sends a negative recommendation regarding a normal node; and Good-mouthing attack where the malicious node sends a positive recommendation regarding a malicious node.

Moreover, the malicious node could behave in various patterns which are:

- Stable malicious behavior: where the malicious node behaves maliciously in continuous manner.
- Non-stable malicious behavior: where the malicious node behaves normally and maliciously in an alternative way. The malicious node changes its behavior with a group of neighbors or during different time periods. Considering this types of attackers is very important because they can gain high trust value [18].

B. System model

Each time the road entity has information to send to the CN, it should go through four phases as follows:

1) Network coverage phase: Each node continuously checks its connectivity with the CN and other nodes.

2) Communication phase: If the source node has a direct link to the CN, it sends the packet directly through the network. Otherwise, the source node sends its packets to a trusted relaying node.

3) Trust calculation phase: During trust period, each node computes the trust value for neighboring nodes. This phase is explained in details in the following Section.

4) Decision phase: Each node has a local blacklist which contains all untrusted neighboring nodes.

III. Recommendation-based trust model for V2X

The proposed model is designed to protect V2X communication against internal attacks. Trust calculations are executed in a distributed manner using weighted-sum method. Building on a comprehensive review in [2], we found that weighted sum and fuzzy logic are the most common methods to measure trustiness in vehicular networks. Furthermore, in our previous work [19], we proposed a comparison between the trust methods for the vehicular network scenario. These results showed that the weighted-sum is more efficient than fuzzy logic.

The trust calculation includes two main trust components as follows:

A. Current Trust - $T^{(t)}_{c(i,j)}$

It is an evaluation of the direct interaction between node i and node j during the time interval t. It is a combination of direct trust and past trust. It is computed using

$$T^{(t)}_{c(i,j)} = \frac{T^{(t)}_{p(i,j)} + T^{(t)}_{d(i,j)}}{2} \tag{1}$$

where $T^{(t)}_{p(i,j)}$ is the past trust measure of node i regarding node j, and $T^{(t)}_{d(i,j)}$ is the direct trust value between node i and node j. The past trust has the same importance as direct trust because we study the impact of non-stable malicious behaviour where past behaviour should be considered. As the compromised node could behave normally in the current time interval (high direct trust), however, it made malicious behaviour during the previous interval (low past trust). Here is the detailed description:

1) Past trust - $T^{(t)}_{p(i,j)}$: It is a measure of the historical behavior of each node j. Indeed, smart attackers behave normally and maliciously sequentially to escape from the punishment. As a result, considering the past behavior of node j is recommended. It is calculated by

$$T^{(t)}_{p(i,j)} = T^{(t-\Delta)}_{g(i,j)} \tag{2}$$

where Δ is the time between two consecutive trust intervals, and $T_{g(i,j)}$ is the global trust value during the previous trust interval $(t-\Delta)$.

2) Direct trust - $T^{(t)}_{d(i,j)}$: Node i computes the direct trust of its one-hop neighboring nodes j which is based on the direct interactions between them. Thus, it is calculated only when there is direct communication between node i and node j at time t. During the interaction, node i collects information regarding the sent packets and whether node j relayed them or not. Therefore, it uses the collected information to compute the direct trust value which represents the forwarding packet rate during the time interval t. It is calculated using

$$T^{(t)}_{d(i,j)} = \frac{Successful\_Interactions}{Total\_Interactions} \tag{3}$$

B. Indirect Trust - $T^{(t)}_{in(i,j)}$

Node i sends requests to the neighboring nodes k to collect their recommendations regarding $node\ j$. Indirect trust is a distributed operation where all nodes can compute indirect trust based on the received recommendations at time t. To achieve an accurate result, the recommender node k should only send its recommendation about node j if it had a previous communication with it. To filter out the dishonest recommendations, we propose the following steps:

1) Confidence value - $C^{(t)}_{(i,k)}$: Node i computes the confidence value for each recommender node k depending on the global trust value $T^{(t)}_{g(i,k)}$. In this case, the recommendations which are sent by malicious nodes could be ignored. The confidence value is computed by

$$C^{(t)}_{(i,k)} = \begin{cases} 1, & \text{if } T^{(t)}_{g(i,k)} \geq Th_C. \\ 0.8, & \text{if } Th_T \leq T^{(t)}_{g(i,k)} < Th_C. \\ 0, & \text{if } T^{(t)}_{g(i,k)} < Th_T. \end{cases} \tag{4}$$

where Th_C is the confidence threshold, and Th_T is the trust threshold. As much as the value 0.8 decreases, lower weight is given for the recommendations from trusted nodes ($Th_T \leq T^{(t)}_{g(i,k)}$). The impact was discussed in our previous work [20].

2) Recommendations clustering: After the node i receives the recommendations, it will divide them into two groups which are positive and negative recommendations. The recommendation is considered positive when $T^{(t)}_{g(i,k)} \geq Th_T$. Otherwise, it is considered a negative recommendation. The proposed recommendation collection process works as shown in Algorithm 1. The average value of the positive recommendations is calculated using

$$P^{(t)}_{(i,j)} = \frac{\sum_{k=1}^{n}[C^{(t)}_{(i,k)} \times T^{(t)}_{g(k,j)}]}{n} \tag{5}$$

and the average value of the negative recommendations is computed by

$$N^{(t)}_{(i,j)} = \frac{\sum_{k=1}^{m}[C^{(t)}_{(i,k)} \times T^{(t)}_{g(k,j)}]}{m} \tag{6}$$

where n and m are the number of positive and negative recommendations respectively.

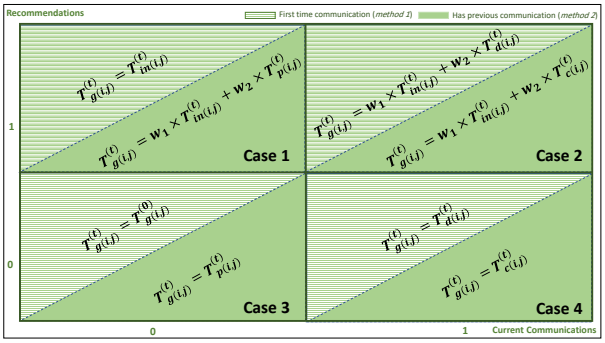


Fig. 1: Global trust decision mapping

3) Indirect trust measure: Node i calculates the indirect trust for node j using

$$T^{(t)}_{in(i,j)} = \alpha \times P^{(t)}_{(i,j)} + \beta \times N^{(t)}_{(i,j)} \tag{7}$$

where α and β are the weights for $P^{(t)}_{(i,j)}$ and $N^{(t)}_{(i,j)}$ respectively, and $\alpha + \beta = 1$. An adaptive weight is applied where α and β are computed based on the number of positive and negative recommendations as follows

$$\alpha = \frac{n}{n+m}, \beta = \frac{m}{n+m}. \tag{8}$$

Because of the impact of confidence value ($C^{(t)}_{(i,k)}$), receiving high number of positive recommendations from untrusted nodes could lead to very low average positive recommendation value. Thus, computing of indirect trust is not only affected by the weights. Also, the indirect trust value is weighted based on the percentage of recommenders. All these factors have impact on indirect trust as this value could be affected by good-mouthing and bad-mouthing attacks. The analysis in Section IV-B on page 6 explained that few positive recommendations from trusted nodes have an impact on the global trust to make a correct decision.

C. Global Trust - $T^{(t)}_{g(i,j)}$

Node i is able to make a decision regarding nearby nodes based on the global trust value. Because the vehicular network has a dynamic topology, the node i experiences various communication cases. Therefore, node i examines three parameters before calculating global trust value for node j as follows:

- New communication: which determines whether the connection between node i and node j is for the first time.
- Existing of recommendations: which checks whether the neighboring nodes of node i have recommendations regarding node j.
- Current communication: which determines if there is a communication between node i and node j during the current interval.

The evaluation of the global trust can be done using Fig.1, where we consider all possible scenarios in V2X communications as follows:

Algorithm 1 Algorithm for collecting recommendations

Input: $Th_T, Th_C, L \leftarrow$ list of node i neighbors which have a previous direct communication with node j
Output: $P^{(t)}_{(i,j)}, N^{(t)}_{(i,j)}$

for each node L(k) **do**
  if $T^{(t)}_{g(i,L(k))} \geq Th_C$ **then**
    $C^{(t)}_{(i,L(k))} \leftarrow 1$
  else
    if $T^{(t)}_{g(i,L(k))} \geq Th_T$ **then**
      $C^{(t)}_{(i,L(k))} \leftarrow 0.8$
    else
      $C^{(t)}_{(i,L(k))} \leftarrow 0$
    end if
  end if
  if $T^{(t)}_{g(L(k),j)} \geq Th_T$ **then**
    $P^{(t)}_{(i,j)} \leftarrow P^{(t)}_{(i,j)} + (C^{(t)}_{(i,L(k))} \times T^{(t)}_{g(L(k),j)})$
    $n \leftarrow n + 1$
  else
    $N^{(t)}_{(i,j)} \leftarrow N^{(t)}_{(i,j)} + (C^{(t)}_{(i,L(k))} \times T^{(t)}_{g(L(k),j)})$
    $m \leftarrow m + 1$
  end if
end for
$P^{(t)}_{(i,j)} \leftarrow \frac{P^{(t)}_{(i,j)}}{n}$
$N^{(t)}_{(i,j)} \leftarrow \frac{N^{(t)}_{(i,j)}}{m}$

- *Case 1: There is no current communication BUT there are recommendations.*
- *Case 2: There are current communications AND recommendations.*
- *Case 3: There is no current communication AND no recommendations.*
- *Case 4: There are current communications BUT no recommendations.*

Depending on whether previous communications exist, global trust is updated using two different methods:

1) Method 1: when node i establishes the communication with node j for the first time. In this scenario, the current trust is ignored because node i does not have an accurate value of node j past behavior. Thus, we only consider the direct and indirect trust. Global trust is measured by

$$T^{(t)}_{g(i,j)} = \begin{cases} T^{(t)}_{in(i,j)}, & \text{Case 1.} \\ w_1 \times T^{(t)}_{in(i,j)} + w_2 \times T^{(t)}_{d(i,j)}, & \text{Case 2.} \\ T^{(0)}_{g(i,j)}, & \text{Case 3.} \\ T^{(t)}_{d(i,j)}, & \text{Case 4.} \end{cases} \tag{9}$$

In case 1, we only consider indirect trust because node i only has recommendations regarding node j. While, when the current communication exists in case 2, node i evaluates node j based on a weight-sum of direct and indirect trust. In case 3, node i does not have any information about node j. Thus, initial global trust value is used. Finally, direct trust is only evaluated in case 4 because of lacking enough recommendations about node j.

2) Method 2: when node i has previous communications with node j. Thus, node i has an updated value for past trust of node j. In this scenario, we consider current trust when direct trust has value. Otherwise, the past trust and indirect trust are measured only. Global trust is computed using

$$T^{(t)}_{g(i,j)} = \begin{cases} w_1 \times T^{(t)}_{in(i,j)} + w_2 \times T^{(t)}_{p(i,j)}, & \text{Case 1.} \\ w_1 \times T^{(t)}_{in(i,j)} + w_2 \times T^{(t)}_{c(i,j)}, & \text{Case 2.} \\ T^{(t)}_{p(i,j)}, & \text{Case 3.} \\ T^{(t)}_{c(i,j)}, & \text{Case 4.} \end{cases} \tag{10}$$

where w_1 and w_2 are weights for indirect trust and (direct/current or past) trust, respectively. w_1 represents the recommendation rate as follows:

$$RW = \frac{0.5}{Neighbors^{(t)}} \tag{11}$$

$$w_1 = (m+n) \times RW \tag{12}$$

where $Neighbors^{(t)}$ is the number of node i neighbors at time t, and $w_2 = 1 - w_1$. When there are no neighbouring nodes, there is no communication established at that period with surrounding entities. Thus, there is no need to compute the trust value where the main aim for trust model is to evaluate the neighbouring nodes behaviour.

Because there are recommendations regarding node j in case 1, node i is able to compute a weighted-sum of indirect and past trust. On the other hand, when the current communication is established in case 2, node i can measure current trust and indirect trust. In case 3, node i can only compute past trust value of node j. Current trust is only considered in case 4 when there are no recommendations regarding node j.

D. Trust decision

Every node has a local blacklist which contains a list of malicious nodes based on its decision. Thus, node i avoids the communication with any node j in the blacklist. Based on $T^{(t)}_{g(i,j)}$, the decision is made by

$$Decision = \begin{cases} Trusted, & \text{if } T^{(t)}_{g(i,j)} \geq Th_T. \\ Malicious, & \text{if } T^{(t)}_{g(i,j)} < Th_T. \end{cases} \tag{13}$$

IV. Simulation Analysis

A. Network specifications

In our simulations, we considered a V2X network with 24 road entities and two RSUs with parameters as shown in Table I. As shown in Fig.2, the road entities move over an area of $900 \times 900\ m^2$ with various speed ranges. The road entity only uses the multi-hop route when it is located out of the network coverage. Therefore, computing trust value for the neighboring nodes in this scenario is a challenge because the node does not continuously communicate with the neighboring nodes.

In addition, the considered network has heterogeneous nodes where the road entity is not limited to vehicles but also includes pedestrian, motorcycles and cycles with various speeds as shown in TABLE II. Thus, the connection time could vary depending on the speed of source and destination nodes.

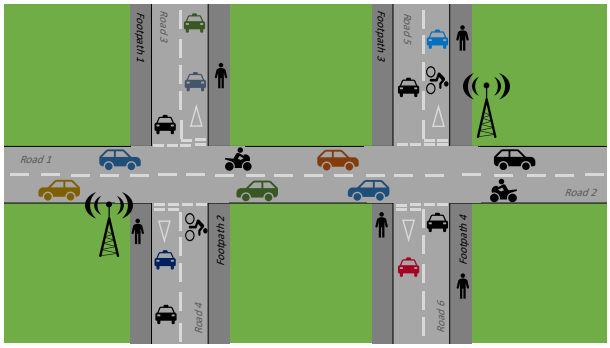


Fig. 2: Simulation area

TABLE I: Simulation Parameters

Parameter	Value
Simulation time (T)	80 iteration
Simulation area	900 × 900
Number of nodes	24
Th_T	0.5
Th_C	0.8
$T^{(0)}_{g(i,j)}$	0.5

TABLE II: Mobility Parameters

Road entity	speed range (mph)
Vehicle	10-30
Pedestrian	0-8
Cycle	3-10
Motorcycle	10-30

To measure the performance of the proposed trust model. We studied four malicious behaviors: blackhole attack, greyhole attack, bad mouthing attack and good mouthing attack.

B. Results

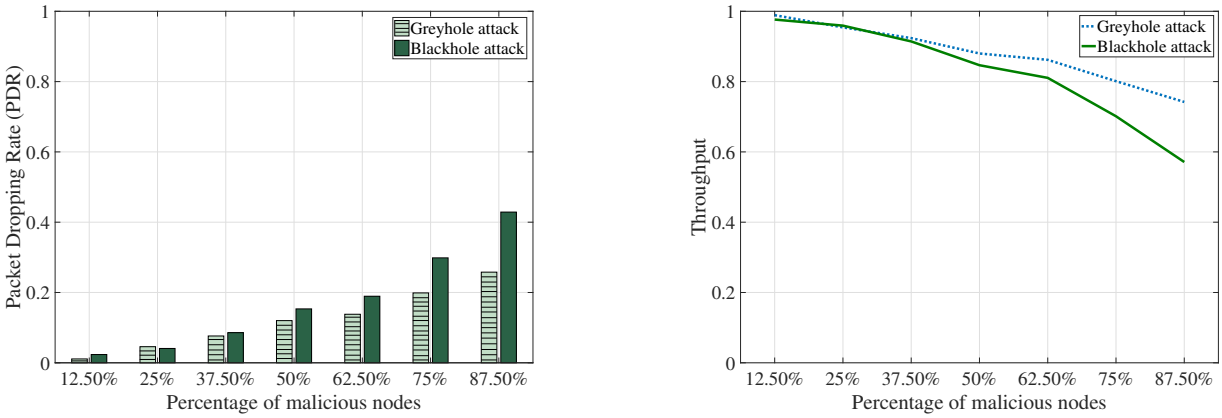
1) Network Performance: The performance of the entire network is represented by two parameters, which are PDR and network throughput, in the presence of malicious nodes. Network throughput is measured by the percentage of packets that are sent successfully. It is calculated using

$$Network\_Throughput = \frac{SP}{TP} \tag{14}$$

where SP is the number of packets that are successfully sent and TP is the total number of generated packets in the network.

In Fig.3 (a), the PDR keeps increasing until reach approximately 0.4 in the worst case when malicious node percentage is more than or equal to 87.50% and all malicious nodes are blackhole attackers where they drop all of the received packets. On the other hand, in the greyhole attack, the dropping rate also increases but at a lower rate.

Moreover, we measured the network throughput as shown in Fig.3 (b) and we notice that our model, in case of greyhole



(a) Packet Dropping Rate (PDR)

(b) Network throughput

Fig. 3: Network Performance in the presence of malicious nodes: a) Packet Dropping Rate; b) Network throughput

attack, can keep the value of throughput greater than 0.7 even in case of the high percentage of malicious nodes. While in the blackhole attack, the network performance decreases to reach 0.65 in the worst case.

2) Detection Rate for Blackhole/Greyhole attackers: Blackhole attack is easier to detect than greyhole attack because the malicious node drops all of the received packets. In Fig.4, we see that the trust value starts with the initial value which is equal to 0.5. In blackhole attack, at the first intervals when the malicious behavior is launched, the trust value drops to 0.08 which is a little value; then, trust value gradually decreases with time. In the greyhole attack, during the first intervals, trust value increases because of a low dropping rate; then, trust value goes down because of the impact of the received recommendations.

3) Analysis for minimum required trustworthy neighbors: As indirect trust is evaluated based on neighboring nodes' recommendations, we analyse the minimum number of trustworthy neighbors to make correct decisions. Also, the existing of recommendation attackers could disturb the trust decisions. In Fig. 5, we present the global trust values in the proposed four cases when indirect trust is calculated (case 1 and case 2 in both methods). In this scenario, the node i evaluates node j (normal node). Then, trusted neighboring nodes s send good recommendations regarding node j ($T^{(t)}_{g(s,j)} \geq 0.6$). However, untrusted nodes k send bad recommendations regarding node j to disturb the decision ($T^{(t)}_{g(s,j)} < 0.5$). As the node j is a normal node, then ($T^{(t)}_{p(i,j)} \geq 0.5$, $T^{(t)}_{d(i,j)} \geq 0.8$). Generally, we notice that the minimum number of neighboring trusted nodes is around 30% of the recommenders to be able to make correct decisions with the existing of recommendation attackers. The following remarks are concluded:

- In case 1-method 1, the global trust is very low and affected by the received recommendations where indirect trust is only considered. The global trust value is above the trust threshold when the percentage of trusted nodes is above 60%.
- In case 1- method 2, the trust value is higher than the previous case because of the impact of past trust in the weighted-sum equation. The value is above the trust threshold when the percentage of trusted nodes is higher than 30%.
- In case 2 – method 1, the global trust records the highest value because the equation is a weighted-sum of direct and indirect trust values. As the direct trust is based on the direct experience, then, the normal node j has a very high value. Thus, the global trust is above the trust threshold when the percentage of trusted nodes is higher than 10%.
- In case 2 – method 2, the global trust is affected by the indirect and current trust (a combination of direct and past trust). Thus, the global trust value goes above the trust threshold when the percentage of trusted nodes is above 20%.

V. Theoretical Analysis

We use the recommendation-based trust model in [14] as a benchmark to evaluate the performance of the proposed model. The model in [14] considered two trust components which are direct and indirect to filter out bogus recommendations. Total trust is computed by

$$T_{ij} = w_d \times T^d_{ij} + w_i \times T^i_{ij} \tag{15}$$

where T^d_{ij} is direct trust, T^i_{ij} is indirect trust. w_d and w_i are the weights for direct and indirect trust respectively, and $w_d + w_d = 1$.

A. Case study 1: Detecting non-stable malicious behavior

Malicious nodes can escape the punishment by stopping its malicious behavior for a while. As a consequence, we measure the ability of malicious node to return after a period of time t as a normal node.

Statement 1. Higher detection rate for non-stable malicious nodes in the proposed model than the existing one.

Proof. The *existing model* applied decay factor (μ) on the number of interactions between node i and node j. The number of positive and negative interactions decreased with

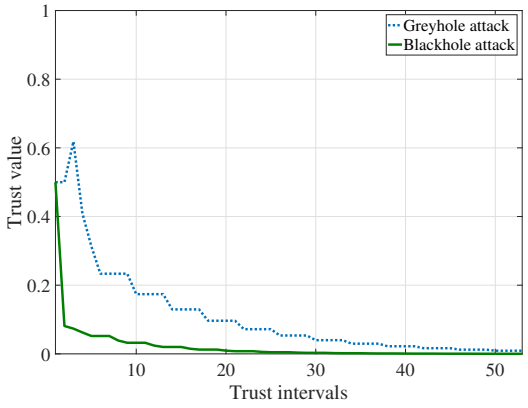


Fig. 4: Trust values for various malicious attacks

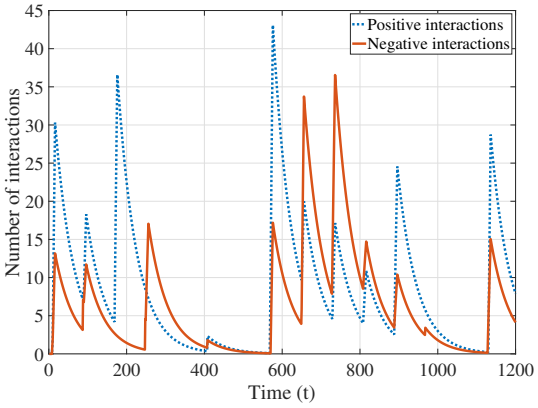


Fig. 6: Effect of decay factor

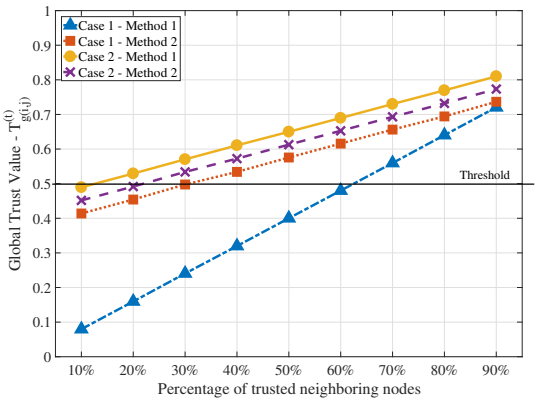


Fig. 5: Analysis for minimum required trustworthy neighbors for make a correct decision regarding normal node j

time when there is no interaction between them as shown in Fig.6. We notice that the number of positive and negative interactions is increased as long as there is a communication between the two nodes. Otherwise, the number of interactions is decreased because of applying the following computation

$$\rho = \rho^{old} \times \mu, \quad \eta = \eta^{old} \times \mu$$

where ρ and η are the number of positive and negative interactions respectively, and $0 \leq \mu \leq 1$. On the other hand, in the *Proposed model*, the global trust always considers past trust when there is a previous communication with the considered node j as shown in eq.(10). In this case, even if the malicious node leaves the area for a while to wash its past behavior. Our proposed model is able to remember its past behavior.

B. Case study 2: Rejecting recommendations from malicious recommenders

In this case, we study the ability of node i to ignore the recommendations which are sent by malicious nodes.

Statement 2. The proposed trust model is able to reject the recommendations from malicious nodes.

Proof. In the *existing model*, we evaluate the ability of the existing model to ignore the recommendations from malicious nodes. The model applied various conditions on the collected recommendations, however, we show that the node may count recommendations from malicious nodes.

First condition is based on the confidence value which is computed by

$$V_{ik}^{conf} = 1 - \sqrt{\frac{12\delta_{ik}\gamma_{ik}}{(\delta_{ik}+\gamma_{ik})^2(\delta_{ik}+\gamma_{ik}+1)}}$$

where δ_{ik} is the accumulative positive interactions between node i and node k, and γ_{ik} is the accumulative negative interactions between node i and node k. They are computed using

$$\delta_{ik} = \rho + 1, \quad \gamma_{ik} = \eta + 1$$

Because the multiplication and summation are reversible operations. Therefore, $V_{if}^{conf1} = V_{if}^{conf2}$ where

$$V_{if}^{conf1} \text{ when } \delta > \gamma \quad \textbf{and} \quad V_{if}^{conf2} \text{ when } \gamma > \delta$$

Then, the confidence value is increased when total number of interactions is increased either positive or negative interactions.

Moreover, the second condition is based on deviation value as follows:

$$|T_{i,j}^{d} - T_{k,j}^{d}| \leq 0.5$$

For example, if node j is a trusted node where $(T_{i,j}^{d} = 1)$. However, node k sends bad recommendation about normal node j where $(T_{k,j}^{d} = 0.5)$. In this case, the deviation condition is achieved and this recommendation is accepted.

On the other hand, in the *proposed model*, during the recommendation collection phase, the node i applies the following conditions on the recommending node k. Thus, if the node k is malicious node, the confidence value $C_{(i,k)}^{(t)}$ is equal to zero and its recommendation is ignored as shown in eq.(4).

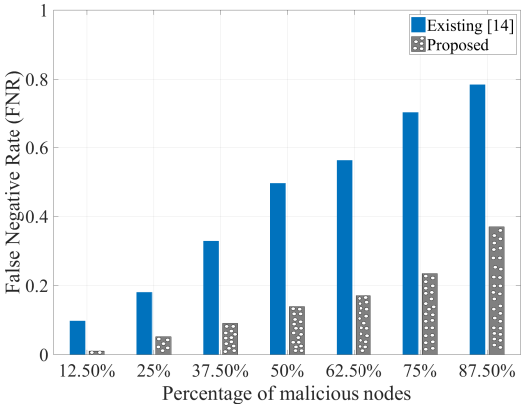


Fig. 7: False Negative Rate

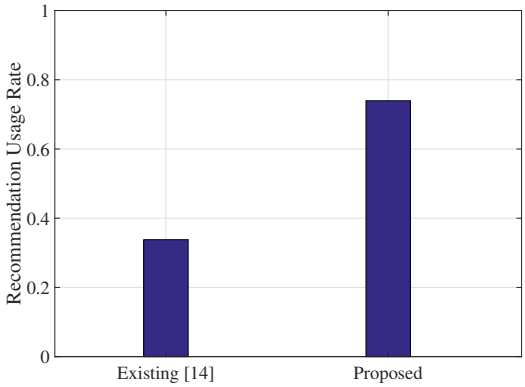


Fig. 8: Recommendation Usage Rate

C. Case study 3: The road entity travels to a new region

In this case, we evaluate the model when the road entity moves from its current location to a new region where there is no previous information about any road entity. We study the ability of the proposed model to make a decision in this case.

Statement 3. The ability of detecting malicious node, when the road entity travels to a new area, in the proposed model is better than the existing model.

Proof. In the *existing model*, the confidence value will be zero for all recommending nodes because the confidence value for them will be as follows.

$$\rho = 0, \quad \eta = 0$$

$$\delta_{ik} = \rho + 1 = 1, \quad \gamma_{ik} = \eta + 1 = 1 \quad \Rightarrow \quad V_{if}^{conf} = 0$$

The algorithm cannot establish trustworthy cluster of recommendations. Therefore, the recommendation system fails and total trust cannot be calculated. If we assume that the model can compute total trust based on the direct trust only, thus, $T_{i,j}^{t} = 0.5$. Therefore, node j is always considered a trusted node because the trust threshold in the existing model is equal to 0.4.

On the other hand, in the *proposed model*, when no previous interactions between node i and node j, we consider the following information:

- $T_{global(i,j)}^{(t)} = T_{indirect(i,j)}^{(t)}$;
- $C_{(i,k)}^{(t)} = 0.8$ because $T_{global(i,k)}^{(t)} = 0.5$ which is the initial value;

We use this information to evaluate the ability of normal node to detect malicious node in a new region.

$$\alpha \times P_{(i,j)}^{(t)} + \beta \times N_{(i,j)}^{(t)} \geq 0.5$$

$$\alpha \times P_{(i,j)}^{(t)} \geq 0.5 - \beta \times N_{(i,j)}^{(t)}$$

$$\alpha \geq \frac{0.8 - \beta \times N_{(i,j)}^{(t)}}{P_{(i,j)}^{(t)}}, \quad \text{where } \beta \times N_{(i,j)}^{(t)} < 0.5$$

The node is trusted only if the value of α is located in the valid range.

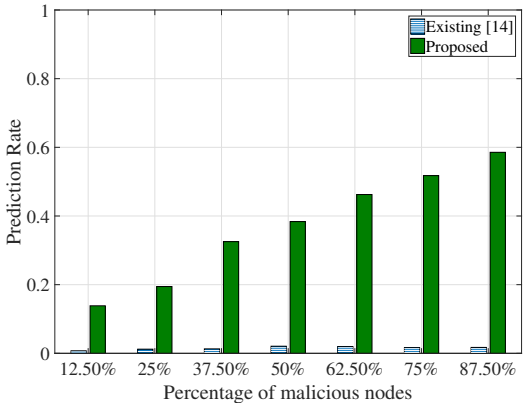


Fig. 9: Prediction Rate

VI. Performance Evaluation

A. Evaluation of Trust Model Performance

1) False Negative Rate: which is the rate of undetected malicious nodes. As much as the model has a low false negative rate, the impact of malicious nodes is minimal. High false negative rate means that the malicious node stays in the network for a long time without being detected. The result that is shown in Fig.7 represents the false negative rate for various percentages of malicious nodes. The following remarks can be made:

- in the existing model, as the percentage of malicious nodes increases, false negative rate rises significantly.
- In comparison with the existing model, the false negative rate is increased slightly in our model. Thus, the malicious node is detected faster in our model than the existing one.
- when the percentage of malicious nodes is high, the false negative rate in the proposed model is still lower than 0.4.

2) Recommendation Usage Rate: is critical in the vehicular network because of the high chance of meeting a new entity. Thus, when the vehicle does not have enough information about the new entity, it leads to wrong decisions. The received recommendations could minimize the incorrect decisions.

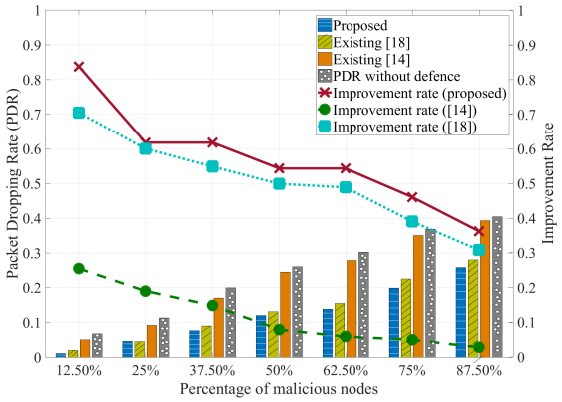


Fig. 10: Improvement Rate in PDR

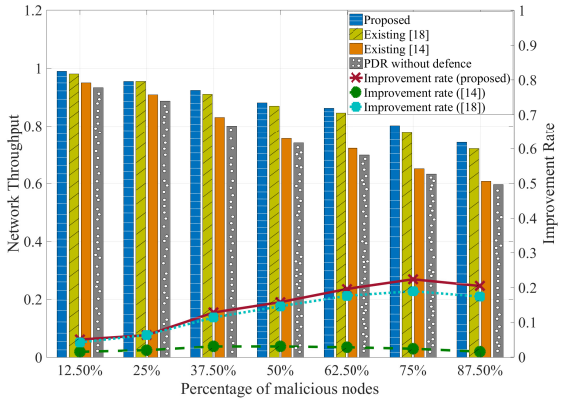


Fig. 11: Improvement Rate in Network Throughput

As a result of the recommendation attacks, the node has to check the trustworthiness of the recommendation source. The node only accepts the recommendations from trusted neighbors. Recommendation usage rate is calculated using

$$Recommendation\_Rate = \frac{Count\_Recommendations}{Total\_Calculations} \tag{16}$$

where $Count\_Recommendations$ is the times of using recommendations in trust calculations and $Total\_Calculations$ is the total number of trust calculations. On the other hand, the existing model [14] applied strict conditions for taking the recommendations which lead to ignore the most of recommendations. Therefore, the recommendation usage rate in the existing model is less than the proposed one as shown in Fig.8, which means that the existing model does not take advantage of using recommendation as much as the proposed model.

3) Prediction Rate: is the rate of avoiding the first communication with malicious nodes. When the node moves to a new location, it needs for the recommendations from the neighboring nodes to have awareness regarding the neighboring malicious nodes and avoid the communication with them. As a result of the high recommendation usage rate in the proposed model, the nodes are able to predict and detect malicious nodes before communicating with them as shown in Fig.9. Thus, it improves the network performance.

B. Evaluation of Network Performance

The performance of the entire network is represented by PDR and network throughput in the presence of malicious nodes. PDR is evaluated to see the impact of such attacks with and without trust models as shown in Fig.10. We notice that the PDR in the proposed model is low in comparison with the network without defence. This clarifies the improvement of the proposed model in the network performance. In addition, the PDR improvement rate in the existing model [18], which applies fuzzy logic method, is very close to the proposed model. On the other hand, PDR for the existing model [14] is very close to the network without defence. Thus, it has a low improvement rate. In addition, PDR in the proposed model is improved to reach 85% when the percentage of malicious nodes is less than or equal to 12.5%.

Moreover, network throughput is measured with and without trust models as shown in Fig.11. We notice that the network throughput in the existing model [18] is very close to the proposed model, however, the proposed model is the highest which leads to an improvement in the network performance. On the other hand, the network throughput for the existing model [14] is very close to the network without defence. In addition, the improvement rate in network throughput in the proposed model is increased when the percentage of malicious nodes is increased.

C. Performance Comparison for Stable malicious behavior

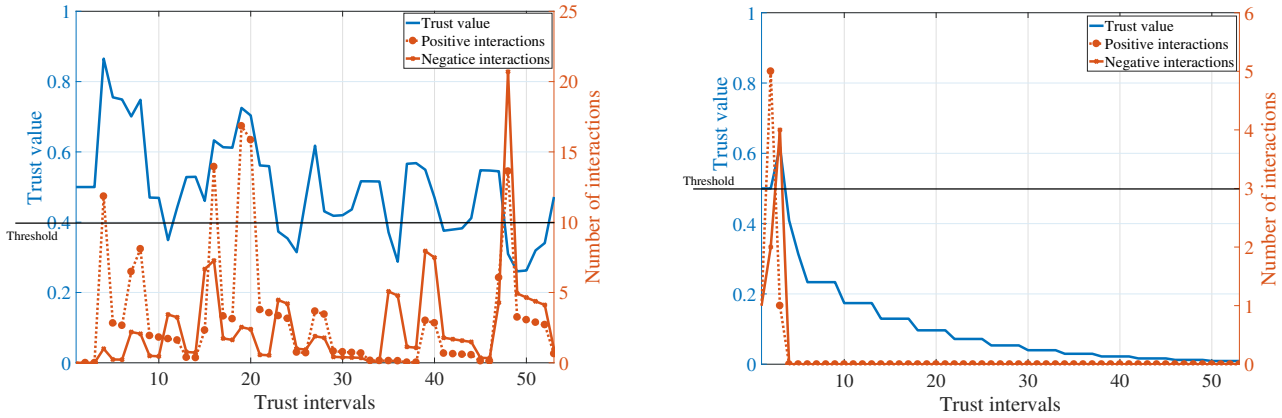
The model performance is studied in the case of stable malicious nodes. From Fig.12 (a), we notice that the trust values are volatile because of the effect of the decay factor. As the number of positive interactions is increased, the trust value rises. In case of no communications for a period, the number of interactions decreases. Thus, the malicious node can return after a while as a normal node, where the trust threshold in the existing mode is equal to 0.4.

On the other hand, we notice that trust value in the proposed model is more consistent than the existing model as shown in Fig.12 (b). At the beginning, the value increases because of the behavior of greyhole attacker. Then, it gradually decreases over the time because when no communication is established for a period, the number of interactions is zero. Thus, the trust value is computed based on the past trust and the recommendations values.

D. Performance Comparison for Non-Stable malicious behavior

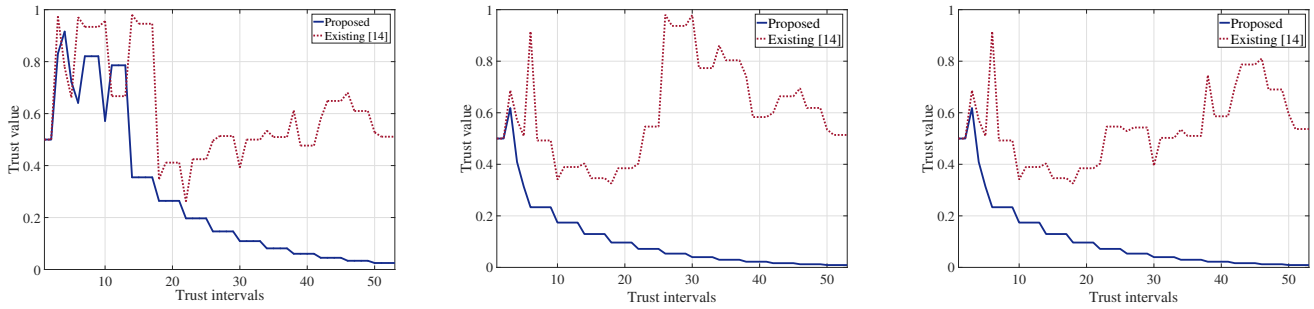
We study the model performance with the existing of non-stable malicious nodes. From the result in Fig.13 we can conclude the following:

- in Fig. 13 (a), the malicious node behaves normally between 1-15 time intervals. We notice that the trust value is increased during these intervals in both models. After the 15^{th} interval, the trust value drops in the



(a) Existing model [14] (b) Proposed model

Fig. 12: Performance Comparison for Stable malicious behavior: a) Existing model [14]; b) Proposed model



(a) Normal behavior between time interval 1 and 15 (b) Normal behavior between time interval 15 and 35 (c) Normal behavior between time interval 35 and 53

Fig. 13: Performance Comparison for Non-Stable malicious behavior

proposed model more than the existing model. The reason for non-steady trust values before the 15^{th} interval is the effect of the recommendations. If the node receives recommendations regarding the malicious node, the trust value goes down. Otherwise, the trust value only depends on the direct experience which means high trust value.

- in Fig. 13 (b), the malicious node behaves normally between 15-35 time intervals. We notice that the normal behavior of the malicious node does not affect the trust value in the proposed model. The reason for that is the impact of past behavior on the trust value. On the other hand, in the existing model, the trust value is gradually increased after 15^{th} interval because of many reasons which are low recommendation usage rate and the impact of the decay factor.
- in Fig. 13 (c), the malicious node behaves normally between 35-53 time intervals. We also notice that the trust value in the proposed model is not affected. However, the trust value is gradually increased after the 35^{th} interval, but it is in a lower value than the previous case.
- in conclusion, our model is less affected by non-stable malicious behavior than the existing model.

VII. Conclusion

In this paper, we proposed a recommendation-based trust model for the V2X network. We conducted various experiments to study the performance of the proposed model. In addition, we considered different malicious attacks which are blackhole attack, greyhole attack, bad mouthing attack and good mouthing attack. Simulation results showed that the proposed model surpasses the existing model. A comparison result showed that our model improves the network performance with 36% when the percentage of malicious nodes is equal to 87.5%. In future work, we will apply the proposed model on a realistic mobility model and compare the results. Also, as autonomous connected vehicles are exposed to physical and cyber attacks [21], we will apply the model on an intra-vehicle communications to protect the sensors.

References

[1] "Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancement for V2X services (3GPP TS 23.285 version 14.2.0 release 14)," ETSI, Tech. Rep., 2017.

[2] A. Alnasser, H. Sun, and J. Jiang, "Cyber security challenges and solutions for V2X communications: A survey," *Computer Networks*, vol. 151, pp. 52–67, 2019.

[3] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: An adversary-oriented overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.
[4] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *Journal of Network and computer Applications*, vol. 35, no. 3, pp. 867–880, 2012.
[5] S. Ahmed and K. Tepe, "Misbehaviour detection in vehicular networks using logistic trust," in *Proc. IEEE Wireless Communications and Networking Conf*, Apr. 2016, pp. 1–6.
[6] C. Laurendeau and M. Barbeau, "Threats to security in DSRC/WAVE," in *International Conference on Ad-Hoc Networks and Wireless*. Springer, 2006, pp. 266–279.
[7] M.-C. Chuang and J.-F. Lee, "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks," *IEEE systems journal*, vol. 8, no. 3, pp. 749–758, 2014.
[8] W. Shen, L. Liu, X. Cao, Y. Hao, and Y. Cheng, "Cooperative message authentication in vehicular cyber-physical systems," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 1, pp. 84–97, 2013.
[9] K. Rostamzadeh, H. Nicanfar, N. Torabi, S. Gopalakrishnan, and V. C. Leung, "A context-aware trust-based information dissemination framework for vehicular networks," *IEEE Internet of Things Journal*, vol. 2, no. 2, pp. 121–132, 2015.
[10] F. G. Mármol and G. M. Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 934–941, 2012.
[11] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A reliable trust-based platoon service recommendation scheme in VANET," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 2, pp. 1786–1797, 2017.
[12] A. Zhou, J. Li, Q. Sun, C. Fan, T. Lei, and F. Yang, "A security authentication method based on trust evaluation in VANETs," *EURASIP Journal on Wireless Communications and Networking*, vol. 2015, no. 1, p. 59, 2015.
[13] S. Ahmed and K. Tepe, "Recommendation trust for improved malicious node detection in ad hoc networks," in *IEEE 86th Vehicular Technology Conference (VTC-Fall)*. IEEE, Sep. 2017.
[14] A. M. Shabut, K. P. Dahal, S. K. Bista, and I. U. Awan, "Recommendation based trust model with an effective defence scheme for MANETs," *IEEE Transactions on Mobile Computing*, vol. 14, no. 10, pp. 2101–2115, 2015.
[15] M. S. Al-Kahtani, "Survey on security attacks in vehicular ad hoc networks (VANETs)," in *Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on*. IEEE, 2012, pp. 1–9.
[16] Y. Al-Raba'nah and G. Samara, "Security issues in vehicular ad hoc networks (VANET): a survey," *International Journal of Sciences & Applied Research (IJSAR)*, vol. 2, no. 4, pp. 50–55, 2015.
[17] J. Zhang, "A survey on trust management for VANETs," in *IEEE international conference on Advanced information networking and applications (AINA)*. IEEE, 2011, pp. 105–112.
[18] A. Alnasser and H. Sun, "A fuzzy logic trust model for secure routing in smart grid networks," *IEEE access*, vol. 5, pp. 17 896–17 903, 2017.
[19] ——, "Performance analysis of behavior-based solutions in vehicular networks," in *Proc. IEEE INFOCOM 2018 - IEEE Conf. Computer Communications Workshops (INFOCOM WKSHPS)*, Apr. 2018, pp. 736–741.
[20] ——, "Global roaming trust-based model for V2X communications," *arXiv preprint arXiv:1909.12381*, 2019.
[21] A. Ferdowsi, S. Ali, W. Saad, and N. B. Mandayam, "Cyber-physical security and safety of autonomous connected vehicles: optimal control meets multi-armed bandit learning," *IEEE Transactions on Communications*, 2019.